giving you a choice
NTUA WIRELESS

February 23, 2016

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W., Suite TW-A325
Washington, D.C. 20554

Re: Annual 64.2009(e) CPNI Certification for 2015
Form 499 Filer ID No. 828872
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to §64.2009(e) of the Commission's rules, NTUA Wireless, LLC, ("NTUAW" or "Company), hereby certifies that the company has established operating procedures that are adequate to ensure compliance with the rules set forth in Subpart U of Part 64 of the Commission's Rules.

NTUAW has not and does not sell any customer information to any company or use such information for purposes of conducting sales and marketing campaigns. NTUAW keeps all customer information and records, whether paper or electronic, in secure locations. Access to these locations and the information stored there are strictly limited.

Attached to this certification is a written policy explaining NTUAW's procedures that ensure compliance with the requirements of the CPNI Rules. The written policy has been distributed to all personnel, and all personnel with access have been trained to maintain customer records as proprietary information and not to share such information with any outside parties.

NTUAW did not take any actions against data brokers in the past year. Also, NTUAW did not receive any customer complaints in the past year concerning unauthorized release of CPNI or experience any confirmed CPNI breaches.

I, the undersigned, certify that I am an officer of NTUAW, and acting as an agent of NTUAW, that I have personal knowledge that NTUAW, has established operating procedures that are adequate to ensure compliance with the Commission's CPNI Rules set forth in §§64.2001 *et seq*.

W. McGill

Wade McGill
Director - NTUAW

Enclosure

CUSTOMER INFORMATION POLICY

This policy outlines how a Customer's personal data should be used and protected.

Personal data includes:

- Personally Identifiable Information (PII)
- Customer Proprietary Network Information (CPNI)
- Credit card information that is contractually regulated by the Payment Card Industry standards (PCI)

PII is any information that allows us to identify a customer. PII includes:

- Name
- Address
- Phone number
- E-mail address
- Social security number (SSN)
- Financial profiles
- Date of Birth

CPNI is information collected by telecommunications companies about Customers' telephone calls. Among other things, this includes the Customer's:

- Bill
- Call detail
- Rate plan
- Minutes of use
- Location

This information must be protected at all times against accidental or unapproved use.

Other personal information that is added to the account during the Customer's relationship with the company must also be protected. This includes:

- Products and services used
- Billing information
- Communications with the company

Only access Customer account information for valid business reasons. Don't access a Customer account:

- For personal reasons
- Out of curiosity
- With no specific business reason

This policy applies to:

- Customers
- Potential Customers
- All company employees
- Any contractor or company that may be given access to the company's data, computer systems, or networks

1. All of the company's data bases that contain customers' personal data must be password protected and access to such data bases must be limited to authorized employees. Distribution of the password must be limited to those authorized employees. The password must be changed regularly and whenever an employee with access to the data and password leaves the company.

2. Customers' personal data should not be removed from the company's offices by employees at any time other than for specific business purposes without the prior approval or without taking the necessary steps to protect such information. This includes computer printouts, handwritten information or notes, copies of files or documents in any electronic form.

3. Authorized employees must closely guard customers' personal data such as customer lists, contact information, telephone numbers, billing information and other customer information to prevent any information from being removed from the company offices by other employees or non-employees either accidentally or intentionally. Authorized employees must ensure they log out of data bases containing customers' personal data and/or lock up such information prior to leaving this information unattended.

4. Any handwritten notes a salesperson, customer care representative or any other employee makes that contain a customer's personal data must be securely filed or shredded at all times and at the end of each business day.

5. Each new customer shall be required to provide the company with certain non-public information that shall be used for identification purposes when the customer calls customer care or any other company employee. Employees must request that the customer verify his/her identity before discussing any matter relating to the customer's personal data. However, customer call detail records can be shared with the customer only by mailing such information to the current billing address associated with account.

6. If the customer visits a retail location in person he/she must be required to provide a valid form of ID before an employee discusses any matter relating to the customer's personal data.

7. CPNI information is never to be used to market any other products or services except services that are related to the service for which the customer already subscribes to. The Company shall maintain a record (electronically or otherwise) of sales and marketing campaigns that use CPNI data for at least one year.

8. As soon as an employee suspects or determines that there has been a breach of CPNI, the employee must immediately notify the Working with Integrity Hotline at 877-331-9079.

9. The company will take action against anyone that violates this policy including but not limited to the following: legal actions, disciplinary actions including termination and/or referrals to law enforcement when appropriate.

10. The Company shall notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

11. The Company shall have an officer sign a compliance certificate on an annual basis and it will be filed with the Commission on or before March 1 for data pertaining to the previous calendar year.